Art. 6 Rechtmäßigkeit der Verarbeitung

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

(2) Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.

(3) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch

a) Unionsrecht oder

b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbe-

zogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. Das Unionsrecht oder das Recht der Mitgliedstaaten müssen ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

(4) Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche – um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist – unter anderem

a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,

b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,

c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,

d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,

e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

Mit der Norm korrespondieren die Erwägungsgründe 10, 32, 39–50.

Literatur: *Abel/Djagani*, Weitergabe von Kreditnehmerdaten bei Forderungskauf und Inkasso, ZD 2017, 114; *Albrecht*, Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung, CR 2016, 88; *Albrecht/Mc Grath/Uphues*, Aufsichtsklausuren aus dem Homeoffice, ZD 2021, 80; *Bach*, Datenschutzrechtliche Vorgaben bei der Weitergabe von Beschäftigten- und Kundendaten während der Due-Diligence-Phase, EuZW 2020, 175; *Behling*, Herausforderung Datenschutz: Rechtskonforme Ausgestaltung von Terrorlisten-Screenings?, NZA 2015, 1359; *Becker*, Consent Management Platforms und Targeted Advertising zwischen DSGVO und ePrivacy-Gesetzgebung, CR 2021, 87; *Becker*, Eine Materialisierung des datenschutzrechtlichen Koppelungsverbots, CR 2021, 230; *Beckers*, Umgang mit Eigentümerdaten, ZWE 2019, 297; *Benecke/Wagner*, Öffnungsklauseln in der Datenschutz-Grundverordnung und das deutsche BDSG – Grenzen und Gestaltungsspielräume für ein nationales Datenschutzrecht, DVBl. 2016, 600; *Bergfink*, Videoüberwachung im öffentlichen Personennahverkehr, Edewecht 2017; *Bieker*, Die Risikoanalyse nach dem neuen EU-Datenschutzrecht und dem Standard-Datenschutzmodell, DuD 2018, 27; *Bock*, Beschränkt Datenschutzrecht die Vertragsgestaltungsfreiheit? – Erforderlichkeit der Verarbeitung i. S. d. Art. 6 Abs. 1 lit. b DSGVO, CR 2020, 173; *Bogenstahl*, Dark Patterns – Mechanismen (be)trügerischen Internetdesigns, Berlin 2019; *Brandt*, Webshops unter DSGVO und ePrivacy-VO, Tracking, Werbung und Informationspflichten, in: Taeger (Hrsg.),

Rechtsfragen digitaler Transformationen – Gestaltung digitaler Veränderungsprozesse durch Recht, Edewecht 2018, S. 1; *Brink*, Digitale Kontaktnachverfolgung soll bei der Pandemie-Bekämpfung helfen, DSB 2021, 138; *Britz/Indenhuck*, Die Daten der Dritten – Verarbeitung drittbezogener Daten im Vertragsverhältnis, in: Taeger (Hrsg.), Rechtsfragen digitaler Transformationen – Gestaltung digitaler Veränderungsprozesse durch Recht, Edewecht 2018, S. 233; *Buchner*, Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, DuD 2016, 155; *Buchner/Schwichtenberg*, Gesundheitsdatenschutz unter der Datenschutz-Grundverordnung, GuP 2016, 218; *Buck-Heeb*, Aufzeichnungspflichten bei Wertpapiergeschäften nach § 83 WpHG, in: Specht-Riemenschneider/Buchner/Heinze/Thomsen (Hrsg.), IT-Recht in Wissenschaft und Praxis, Festschrift für Jürgen Taeger, Frankfurt/M. 2020, S. 111; *Bull*, Netzpolitik: Freiheit und Rechtsschutz im Internet, Baden-Baden 2013*Bull*, Sinn und Unsinn des Datenschutz, Tübingen 2015; *Bunnenberg*, Privatautonomie und Datenschutz, JZ 2020, 1088; *Conrad*, Verarbeitung biometrischer Daten – sind die neuen Geschäftsmodelle zulässig?, K&R 2020, 253; *Culik/Döpke*, Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen, ZD 2017, 226; *Dallmann/Busse*, Verarbeitung von öffentlich zugänglichen personenbezogenen Daten, ZD 2019, 394; *Dammann*, Erfolge und Defizite der EU-Datenschutzgrundverordnung – Erwarteter Fortschritt, Schwächen und überraschende Innovationen, ZD 2016, 307; *Dienstbühl*, Anforderungen an den Einsatz von „Wildkameras" durch Privatpersonen, CR 2019, 359; *Dieterich*, Von Risiken und Nebenwirkungen – Ein Jahr (Online-)Prüfungen in der Corona-Pandemie, NVwZ 2021, 511; *Dix*, Daten als Bezahlung – Zum Verhältnis zwischen Zivilrecht und Datenschutzrecht, ZEuP 2017, 1; *Drewes*, Dialogmarketing nach der DSGVO ohne Einwilligung der Betroffenen, CR 2016, 721; *Dzida*, Neue datenschutzrechtliche Herausforderungen für das Personalmanagement, BB 2019, 3060; *Eggers*, Die Zukunft der Cookies: Die Nutzung von Online-Trackingtechnologien, in: Taeger (Hrsg.), Den Wandel begleiten – IT-rechtliche Herausforderung der Digitalisierung, Edewecht 2020, S. 161; *Eisenschmid,* Datenschutz im Miet- und Wohnungseigentumsrecht, NZM 2019, 313; *Elking*, Terrorscreening, AuA 2016, 604; *Engeler*, Das überschätzte Kopplungsverbot, ZD 2018, 55; *Engeler/Marosi*, Planet49: Neues vom EuGH zu Cookies, Tracking und ePrivacy, CR 2019, 707; *Engelien-Schulz*, Zu den ersten Folgen der EU-Datenschutz-Grundverordnung für öffentliche Stellen, UBWV 2016, 373; *Ettig/Herbrich*, Wird's besser, wird's schlimmer? – Das Online-Marketing zwei Jahre nach dem Wirksamwerden der DSGVO, K&R 2020, 719; *Funke*, Tracking: Zur Sinnhaftigkeit der Einwilligung als Rechtsgrundlage, in: Taeger (Hrsg.), Den Wandel begleiten – IT-rechtliche Herausforderung der Digitalisierung, Edewecht 2020, S. 179; *Galetzka*, Web-Analytics/Retargeting und automatisierte Einzelfallentscheidung, in: Taeger (Hrsg.), Rechtsfragen digitaler Transformationen – Gestaltung digitaler Veränderungsprozesse durch Recht, Edewecht 2018, S. 45; *Gierschmann*, Was „bringt" deutschen Unternehmen die DS-GVO?, ZD 2016, 51; *Giesen*, Totaler Datenschutz in der EU: freiheitswidrig, bürokratisch und erfolglos!, NVwZ 2019, 1711; *Giesen*, Kurzes Plädoyer gegen unser Totalverbot: Deine Daten gehören Dir keineswegs!, PinG 2013, 62; *Glatschke/Mann/Reibach/Ukena*, Datenschutzfreundliches On-Board Fuel Consumption Metering durch entkoppelte Identitäten, in: Taeger (Hrsg.), Im Fokus der Rechtsentwicklung – Die Digitalisierung der Welt, Edewecht 2021, S. 43; *Göpfert/Meyer*, Datenschutz bei Unternehmenskauf: Due Diligence und Betriebsübergang, NZA 2011, 486; *Götz/Götz*, Familienrechtliche Überlegungen zur Corona-Warn-App, FamRZ 2020, 1250; *Gola/Lepperhoff*, Reichweite des Haushalts- und Familienprivilegs bei der Datenverarbeitung, ZD 2016, 9; *Gola/Klug*, Grundzüge des Datenschutzes, München 2003; *Golland*, Das Telekommunikation-Telemedien-Datenschutzgesetz, NJW 2021, 2238; *Grabitz/Hilf/Nettesheim*, Das Recht der Europäischen Union: EUV/AEUV; Stand: 2017, München; *Gräfe*, Webtracking und Microtargeting als Gefahr für Demokratie und Medien, in: Taeger (Hrsg.), Rechtsfragen digitaler Transformationen, 2018, S. 27; *von Grafenstein*, Das Zweckbindungsprinzip zwischen Innovationsoffenheit und Rechtssicherheit, DuD 2015, 789; *Greve*, Das neue Bundesdatenschutzgesetz, NVwZ 2017, 737; *Haase*, Die Einwilligung im Datenschutzrecht – Einschränkung der Freiheit des Einzelnen durch die überzogene Forderung nach Freiwilligkeit, InTeR 2019, 113; *Hacker*, Datenprivatrecht, 2020; *Härting*, Datenschutz und Persönlichkeitsrechte: Verbotsprinzip und offener Tatbestand in: Leible/Kutschke (Hrsg.), Schutz der Persönlichkeit im Internet, Stuttgart/München 2012, S. 55; *Hansen-Oest*, Weitergabe von Kundendaten beim Asset Deal – Einwilligung erforderlich?, DSB 2020, 60; *Härting*, Datenschutz-Grundverordnung, in: Taeger (Hrsg.), IT und Internet – mit Recht gestalten; Edewecht 2012, S. 687; *Härting*, Datenschutzrecht: Verbotsprinzip und Einwilligungsfetisch, AnwBl 2012, 716; *Härting*, Starke Behörden, schwaches Recht – der neue EU-Datenschutzentwurf, BB 2012, 459; *Härting/Schneider*, Das Ende des Datenschutzes –

es lebe die Privatsphäre, Eine Rückbesinnung auf die Kern-Anliegen des Privatsphärenschutzes, CR 2015, 819; *Härting/Schneider*, Das Dilemma der Netzpolitik, ZRP 2011, 233; *Haumann*, Videoüberwachung in Bundesligastadien, in: Taeger (Hrsg.), Rechtsfragen digitaler Transformationen, 2018, S. 73; *Haustein*, Datenschutzrechtskonforme Ausgestaltung von Dashcams und mögliche Ableitungen für den autonomen PKW, in: Taeger (Hrsg.), Smart World – Smart Law? Weltweite Netze mit regionaler Regulierung, Edewecht 2016, S. 43; *Heinzke/Engel*, Datenverarbeitung durch Auftragserfüllung – Anforderungen und Grenzen, ZD 2020, 189; *Heinson*, Datenschutz im Finanzwesen, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, München 2019, § 14; *Herfurth*, Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO, ZD 2018, 514; *Herbrich*, Unterlassungsanspruch hinsichtlich einer mit Gewinnspiel verbundenen Werbung für Inkontinenzhilfsmittel und erfolgter Einholung einer Einwilligung für E-Mail-Werbung, jurisPR-ITR 23/2020 Anm. 5; *Herdes*, Daten im Konzern: Datenschutz im B2C Bereich, in: Taeger (Hrsg.), Rechtsfragen digitaler Transformationen – Gestaltung digitaler Veränderungsprozesse durch Recht, Edewecht 2018, S. 209; *Herting*, LfD Niedersachsen: DSGVO-Einwilligungen auf Websites und Anforderungen an Consent-Layer, DSB 2021, 53; *Hölters*, Handbuch Unternehmenskauf, 9. Aufl., Köln 2019; *Hornung*, Eine Datenschutz-Grundverordnung für Europa?, ZD 2015, 99; *Indenhuck/Britz/Wettlaufer*, Proctoring durch KI – Datenschutzrechtliche Anforderungen an den Einsatz von automatisierter Online-Prüfungssoftware im Hochschulbereich, in: Taeger (Hrsg.), Im Fokus der Rechtsentwicklung – Die Digitalisierung der Welt, Edewecht 2021, S. 499; *Jandt*, Biometrische Videoüberwachung – was wäre wenn …, ZRP 2018, 16; *Janicki*, Die Einwilligungsfähigkeit zwischen Digitalisierung und demographischem Wandel, in: Taeger (Hrsg.), Die Macht der Daten und der Algorithmen, Edewecht 2019, S. 313; *Johnson/Brechtel*, Videoüberwachung und DSGVO: Eine unüberwindbare Herausforderung?, ITRB 2019, 208; *Karg*, Die Renaissance des Verbotsprinzips im Datenschutz, DuD 2013, 75; *Koglin*, Planet49: Praktische Umsetzung der Vorgaben des EuGH zu Cookies und Einwilligungen, DSB 2019, 255; *Kollmar/El-Auwad*, Grenzen der Einwilligung bei hochkomplexen und technisierten Datenverarbeitungen, in: Taeger (Hrsg.), Den Wandel begleiten – IT-rechtliche Herausforderung der Digitalisierung, Edewecht 2020, S. 199; *Korinth*, Datenschutz-Grundverordnung – Was ändert sich für den Betriebsrat?, ArbRB 2018, 47; *Krämer*, Die Rechtmäßigkeit der Nutzung von Scorewerten, NJW 2020, 497; *Krämer*, Die Verarbeitung personenbezogener Daten durch Inkassounternehmen und Auskunfteien nach der DS-GVO, NJW 2018, 347; *Krusche*, Kumulation von Rechtsgrundlagen zur Datenverarbeitung, ZD 2020, 232; *Kühling*, Neues Bundesdatenschutzgesetz – Anpassungsbedarf bei Unternehmen, NJW 2017, 1985; *Kühling/Martini*, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, 448; *Kühling/Schildbach*, Corona-Apps – Daten- und Grundrechtsschutz in Krisenzeiten, NJW 2020, 1545; *Lach*, Datenschutzverstoß als berufsrechtliche Pflichtverletzung des Rechtsanwalts, jurisPR-ITR 22/2018 Anm. 3; *Lachenmann*, Datenübermittlung im Konzern, Edewecht 2016; *Langhanke*, Daten als Gegenleistung, Tübingen 2018; *Laue*, Öffnungsklauseln in der DS-GVO – Öffnung wohin?, ZD 2016, 463; *Lehmann/Wancke*, Abtretung von Darlehensforderungen und Datenschutz – Neues zu einer problematischen Beziehung – Teil 1, WM 2019, 613; *v. Lewinski*, Persönlichkeitsprofile und Datenschutz bei CRM, RDV 2003, 122; *Lüttge*, Unternehmensumwandlungen und Datenschutz, NJW 2000, 2463; *Mackenthun*, Datenschutzrechtliche Voraussetzungen der Verarbeitung von Kundendaten beim zentralen Rating und Scoring im Bank-Konzern, WM 2004, 1713; *von Maltzan/Moshashai*, Incident Response zur Lagebilderstellung, in: Taeger (Hrsg.), Rechtsfragen digitaler Transformationen, 2018, S. 145; *Martini/Drews/Seeliger/Weinzierl*, ZfDR 2021, 47; *Masing*, Herausforderungen des Datenschutzes, NJW 2012, 2305; *Möhrke-Sobolewski/Klas*, Datenschutzkonformes Webtracking, ITRB 2016, 182; *Monreal*, Weiterverarbeitung nach einer Zweckänderung in der DS-GVO, ZD 2016, 507; *Moos*, Update Datenschutz, in: Taeger (Hrsg.), Die Macht der Daten und der Algorithmen – Regulierung von IT, IoT und KI, Edewecht 2019, S. 189; *Moos/Strassemeyer*, Der gestalterische Spielraum für Einwilligungserklärungen nach BGH Cookie-Einwilligung II, DSB 2020, 207; *Nägele/Apel* (Hrsg.), Beck'sche Online-Formulare IT- und Datenrecht, 6. Ed., München 2021; *Nebel*, Die Zulässigkeit der Übermittlung personenbezogener Kundenstammdaten zum Vollzug eines Asset Deal, CR 2016, 417; *Nettesheim/Diggelmann*, Grundrechtsschutz der Privatheit, VVDStRL 2011, 7; *Nelles*, Daten- und Bildnisschutz auf dem Sportplatz, ITRB 2021, 60; *Ory/Weth* (Hrsg.), jurisPK-ERV, Band 1, Saarbrücken, Stand 1/2021; *v. Olenhusen/Crone*, Der Anspruch auf Auskunft gegenüber Internet-Providern bei Rechtsverletzungen nach Urheber- bzw. Wettbewerbsrecht, WRP 2002, 164; *Peifer*, Die Datenschutz-Grundverordnung aus Sicht der öffent-

lichen Verwaltung, PinG 2016, 222; *Peifer*, Verhaltensorientierte Nutzeransprüche – Tod durch Datenschutz oder Moderation durch das Recht? K&R 2011, 543; *Piltz*, „Sicherheit der Verarbeitung" als gesetzlicher Erlaubnistatbestand – Wann dürfen personenbezogene Daten zum Zweck der Daten- und IT-Sicherheit verwendet werden?, in: Specht-Riemenschneider/Buchner/Heinze/Thomsen (Hrsg.), IT-Recht in Wissenschaft und Praxis, Festschrift für Jürgen Taeger, Frankfurt/M., 2020, S. 351; *Piltz/Kühner*, Ausnahme-Vorschriften bei Cookie-Einwilligungen, ZD 2021, 123; *Piltz/Zwerschke*, Die rückwirkende Heilung rechtswidriger Datenverarbeitungen, DSB 2020, 148; *Plath/Struck/ter Hazeborg*, Verkauf von Kundendaten im Asset Deal, CR 2020, 9; *Quiel*, Die Datenschutz-Folgenabschätzung und ihre Durchführung in der Praxis am Beispiel von Werbebildschirmen mit Gesichtserkennungssensorik, PinG 2018, 30; *Reibach*, Datenschutzrechtliche Zulässigkeit von gewerkschaftlichen Direktwerbemaßnahmen gegenüber Nichtmitgliedern, in: Specht-Riemenschneider/Buchner/Heinze/Thomsen (Hrsg.), IT-Recht in Wissenschaft und Praxis, Festschrift für Jürgen Taeger, Frankfurt/M., 2020, S. 361; *Reibach*, Nationales Datenschutzrecht – die Deharmonisierung der DSGVO, in: Taeger (Hrsg.), Rechtsfragen digitaler Transformationen – Gestaltung digitaler Veränderungsprozesse durch Recht, Edewecht 2018, S. 133; *Remmertz*, DSGVO ante portas: Aktuelle Brennpunkte im Online-Marketing, GRUR-Prax 2018, 254; *Riechert*, Daten als Gegenleistung, PinG 2019, 234; *Robrahn/Bremert*, Interessenkonflikte im Datenschutzrecht, ZD 2018, 291; *Rose*, „Smart Cams" im öffentlichen Raum, ZD 2017, 64; *Rose*, Erforderlichkeit und Interessengerechtigkeit der Videoüberwachung im öffentlichen Raum, RDV 2019, 123; *Roßnagel*, Kein „Verbotsprinzip" und kein „Verbot mit Erlaubnisvorbehalt", NJW 2019, 1; *Roßnagel*, Datenschutz-Grundverordnung – was bewirkt sie für den Datenschutz?, vorgänge 221/222 (2018), 17; *Roßnagel*, Gesetzgebung im Rahmen der Datenschutz-Grundverordnung, DuD 2017, 277; *Roßnagel*, Datenschutzgesetzgebung für öffentliche Interessen und den Beschäftigungskontext, DuD 2017, 290; *Rost*, Risiken im Datenschutz, vorgänge 221/222 (2018), 79; *Ruschemeier*, Anforderungen an datenschutzrechtliche Einwilligungen in Krisenzeiten, ZD 2020, 618; *Schaffland*, Datenschutz und Bankgeheimnis bei Fusion (k)ein Thema?, NJW 2002, 1539; *Schantz*, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, 1841; *Schleifenbaum*, Datenschutz oder Tatenschutz in der Versicherungswirtschaft, Berlin 2009; *Schleipfer*, Datenschutzkonformes Webtracking nach Wegfall des TMG, ZD 2017, 460; *Schmidl*, Die Subsidiarität der Einwilligung im Arbeitsverhältnis, DuD 2007, 756; *Schnebbe/Trinks*, Due Diligence – Datenschutzrechtlicher Praxisleitfaden, 2021; *Schneider, J.*, Das Anwaltsgeheimnis im Zeichen von Cloud Computing, ITRB 2011, 243; *Schneider, J.*, Hemmnis für einen modernen Datenschutz: Das Verbotsprinzip, AnwBl 2011, 233; *Schneider, J.*, Überlegungen zu einer Neugestaltung des Datenschutzrechts, ITRB 2012, 180; *Schneider, J./Härting*, Zehn „Navigationsempfehlungen", damit das EU-Datenschutzrecht internettauglich und effektiv wird, CR 2014, 306; *Schneider, M.*, Das Rückgriffsverbot im Datenschutz – kein „best of both worlds"?, CR 2017, 568; *Schneider, N.*, Geltungsdauer einer Einwilligung in die Werbeansprache, in: Taeger (Hrsg.), Rechtsfragen digitaler Transformationen, Edewecht 2018, S. 221; *Schwenke*, Private Nutzung von Smartglasses im öffentlichen Raum, Edewecht 2016; *Schwenke*, Zulässigkeit der Nutzung von Smartcams und biometrischen Daten nach der DS-GVO, NJW 2018, 823; *Selk*, Kundendaten in der Hotellerie, RDV 2008, 187; *Specht*, Das Verhältnis möglicher Datenrechte zum Datenschutzrecht, GRUR Int. 2017, 1040; *Specht*, Daten als Gegenleistung – Verlangt die Digitalisierung nach einem neuen Vertragstypus?, JZ 2017, 763; *Specht*, Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit, in: Briner/Funk (Hrsg.), DGRI Jahrbuch 2017, Köln 2018, S. 35; *Specht/Mantz* (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, München 2019; *Spindler*, Die neue EU-Datenschutz-Grundverordnung, DB 2016, 937; *Spindler*, Persönlichkeitsschutz im Internet, Gutachten F zum 69. DJT, München 2012; *Spittka*, Der Unternehmensbegriff der DS-GVO, in: Taeger (Hrsg.), Rechtsfragen digitaler Transformationen – Gestaltung digitaler Veränderungsprozesse durch Recht, Edewecht 2018, S. 119; *Steinrötter*, Datenschutzrechtliche Implikationen beim Einsatz von Pflegerobotern, ZD 2020, 336; *Stentzel*, Der datenschutzrechtliche Präventionsstaat, PinG2016, 45; *Storm*, Datenschutz-Grundverordnung, DWW 2018, 204; *Strauß*, Dashcam und Datenschutz, NZV 2018, 554; *Suwelack*, Datenschutz in Unternehmenstransaktionen – Die DSGVO als Dealbreaker?, in: Taeger (Hrsg.), Den Wandel begleiten – IT-rechtliche Herausforderung der Digitalisierung, Edewecht 2020, S. 271; *Taeger/Kremer*, Recht des E-Commerce und Internet, 2. Aufl. 2021; *Taeger*, Datenschutz im Versandhandel: Übermittlung von Kundendaten mit positivem Bonitätswert, BB 2007, 785; *Teichmann/Kiessling*, Datenschutz bei Umwandlungen, ZGR 2001, 33; *Tinnefeld*, Die selbstbestimmte Einwilligung – Bedeutung, Möglichkeiten und Grenzen, vorgänge 221/

222 (2018), 41; *Tinnefeld/Conrad*, Die selbstbestimmte Einwilligung im europäischen Recht, ZD 2018, 391; *Ueberfeldt*, Cyber Security – neue Wege für Analytics und Produktentwicklung?, in: Taeger (Hrsg.), Rechtsfragen digitaler Transformationen – Gestaltung digitaler Veränderungsprozesse durch Recht, Edewecht 2018, S. 729; *Uebersalz*, Regulierung der Hochschulförderung durch Private zur Korruptionsprävention, Edewecht 2017; *Uecker*, Die Einwilligung im Datenschutzrecht und ihre Alternativen, ZD 2019, 248; *Veil*, Einwilligung oder berechtigtes Interesse? – Datenverarbeitung zwischen Skylla und Charybdis, NJW 2018, 3337; *Veil*, DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip – eine erste Bestandsaufnahme, ZD 2015, 347; *Veil*, Die Datenschutz-Grundverordnung: des Kaisers neue Kleider – Der gefährliche Irrweg des alten wie des neuen Datenschutzrechts, NVwZ 2018, 686; *Voigt*, Konzerninterner Datentransfer, CR 2017, 429; *Voigt/Herrmann/Danz*, Die elektronische Signatur und ihre Einsatzmöglichkeiten für digitale Vertragsschlüsse, NJW 2020, 2991; *Weberling*, Rechtsfragen bei der Einführung von Kundenkarten, AfP 2004, 397; *Wehkam*, Weiterverarbeitung zu anderen Zwecken: Praktische Kompatibilitätsprüfung bei Zwischenspeicherung für Zweckfremde Datenanalysen, in: Taeger (Hrsg.), Den Wandel begleiten – IT-rechtliche Herausforderung der Digitalisierung, Edewecht 2020, S. 215; *Wehmeyer*, Datenschutz-Grundverordnung und Unternehmenstransaktionen – Was gilt zukünftig für den Umgang mit Kundendaten?, PinG 2016, 215; *Weichert*, Von Gästelisten, Luca und der CWA, CuA 2021, Nr. 6, 27; *Weichert*, Wider das Verbot mit Erlaubnisvorbehalt im Datenschutz?, DuD 2013, 246; *Weichert*, Datenschutz als Verbraucherschutz, DuD 2001, 264; *Weinzierl*, NVwZ-Extra, 1/2020, 1; *Wengert/Widmann/Wengert*, Bankenfusionen und Datenschutz, NJW 2000, 1289; *von Westphalen*, Verzweifelte Suche nach der verlorenen Vertragsfreiheit, ZIP 2020, 437; *von Westphalen/Wendehorst*, Hergabe personenbezogener Daten für digitale Inhalte, BB 2016, 2179; *von Westphalen/Wendehorst*, Der Entwurf neuer Leitlinien des Europäischen Datenschutzausschusses 2/2019 betreffend die Auslegung von Art. 6 Abs. 1 lit. b DSGVO, ZIP 2019, 1937; *Wilfling*, Die datenschutzrechtlichen Anforderungen an Cookie Einwilligungen – Das Ende der Cookie Banner?, in: Taeger (Hrsg.), Die Macht der Daten und der Algorithmen – Regulierung von IT, IoT und KI, Edewecht 2019, S. 301; *Wurzberger*, Anforderungen an Betriebsvereinbarungen nach der DS-GVO, ZD 2017, 258; *Wybitul/Sörup/Pötters*, Betriebsvereinbarungen und § 32 BDSG: Wie geht es nach der DS-GVO weiter?, ZD 2015, 559; *Zetzsche*, Datenschutz und Hauptversammlung, AG 2019, 233.

Übersicht

I. Allgemeines

1. Bedeutung der Vorschrift

Aus Art. 8 Abs. 2 Satz 1 GRCh folgt, dass personenbezogene Daten von hoheitlichen Stellen nur „mit Einwilligung der betroffenen Person oder auf einer sonstigen *gesetzlich geregelten legitimen Grundlage* verarbeitet“ werden dürfen.[1] Als primären Grundsatz der Verarbeitung personenbezogener Daten verlangt auch Art. 5 Abs. 1 lit. a DSGVO, dass personenbezogene Daten – von staatlichen wie privaten Stellen – nur *rechtmäßig* verarbeitet werden und nach Buchstabe b auch nur „für festgelegte, eindeutige und *legitime* Zwecke“ erhoben worden sein dürfen.[2] Hieran knüpft Art. 6 DSGVO an. Schon die Überschrift „Rechtmäßigkeit der Verarbeitung“ bringt dies zum Ausdruck. Art. 6 Abs. 1 UAbs. 1 **1**

1 Siehe zur „Zur Dogmatik der Datenverarbeitung als Grundrechtseingriff“ mit Erläuterung der für den Datenschutz verfassungsrechtlichen Relevanz von Artt. 7 und 8 GrCh und des für die verfassungsrechtliche Bewertung des BDSG und anderer nationaler Datenschutzvorschriften noch relevanten Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (Recht auf informationelle Selbstbestimmung) *Roßnagel*, NJW 2019, 1.

2 Die Verwendung des Terminus „legitim“ sowohl in Art. 8 Abs. 2 Satz 1 GRCh („auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet“) als auch in Art. 5 Abs. 1 lit. b DSGVO weist darauf hin, dass die Rechtsgrundlage selbst verfassungsgemäß sein muss. Die Datenverarbeitung bedarf nicht nur eines Erlaubnistatbestands, sondern es ist zu gewährleisten, dass der Zweck nicht von der Rechtsordnung missbilligt wird; siehe dazu *Specht*, GRUR Int. 2017, 1040, 1042, m. w. N., sowie pointiert *Rost*, vorgänge 221/222 (2018), 79, 84 f.

DSGVO listet die in Betracht kommenden **Erlaubnistatbestände** auf, aus denen sich die Rechtmäßigkeit der Verarbeitung ergeben kann. Über die in Abs. 1 UAbs. 1 lit. a bis f aufgeführten Rechtmäßigkeitsalternativen hinaus kann es allerdings spezifische Regelungen im Unionsrecht oder im Recht der Mitgliedstaaten aufgrund einer in der DSGVO enthaltenen Öffnungsklausel geben.[3]

2 Weitere mitgliedstaatliche Datenschutzvorschriften mit fachspezifischen Erlaubnistatbeständen für die Verarbeitung personenbezogener Daten finden sich darüber hinaus dann, wenn sie der Umsetzung einer fachspezifischen Richtlinie wie beispielsweise der RL 2016/680 (Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung) oder RL 2002/58/EG (E-Privacy-Richtlinie) dienen. Nationales Datenschutzrecht findet sich auch, wenn der Mitgliedstaat eine Datenschutzvorschrift mit Erlaubnistatbestand auf einem Gebiet verabschiedet, auf dem die EU nach dem AEUV keine **Regelungskompetenz** besitzt. Insofern kann nicht die Rede davon sein, dass Art. 6 DSGVO die Erlaubnistatbestände für die Verarbeitung personenbezogener Daten abschließend regelt.[4] Damit bleibt es bei der aus dem nationalen Datenschutzrecht bekannten Situation, dass sich auch aus dem allgemeinen Datenschutzrecht, bestehend aus **BDSG** und **Landesdatenschutzgesetzen**, und den **fachspezifischen Datenschutzgesetzen** Erlaubnistatbestände ergeben können. Es gilt auch unter der DSGVO, dass stets zu prüfen ist, ob für eine Datenverarbeitung (neben oder statt der DSGVO) andere Datenschutzvorschriften zur Anwendung kommen, aus denen sich eine Erlaubnis für die Verarbeitung personenbezogener Daten ergeben können. Darunter sollte nach einer Mitteilung des BMI[5] auch § 23 KUG fallen, der Ausnahmen vom Verbot der **Verarbeitung von Bildnissen** vorsieht. Nach einer Entscheidung des BGH[6] findet das KUG allerdings aufgrund der Öffnungsklausel des Art. 85 Abs. 2 DSGVO nur für eine Verarbeitung von Bildnissen im journalistischen Bereich Anwendung. Die §§ 22, 23 KUG stellen Regelungen zur Umsetzung des **Medienprivilegs** dar.

3 Es besteht demzufolge weiter eine große Zahl von Gesetzen, die in dem 1. Anpassungsgesetz des Bundes[7] mit dem BDSG als Artikel 1 und dem 2. Gesetz zur Anpassung des Datenschutzrechts[8] aufgeführt sind und Erlaubnistatbestände enthalten oder die sich aus **Anpassungsgesetzen** der Länder ergeben oder, ohne in Anpassungsgesetzen erwähnt zu werden, aufgrund von **Öffnungsklauseln** weiter gelten oder neu verabschiedet werden. Es kann deshalb kaum die Rede davon sein, dass die DSGVO zu einer Vereinheitlichung des Daten-

---

3 Zu den hier angesprochenen Regelungen zählen nicht nur Gesetze im formellen Sinn, sondern aufgrund von Art. 88 DSGVO auch weiterhin Betriebsvereinbarungen, siehe jetzt *Korinth*, ArbRB 2018, 47; *Wurzberger*, ZD 2017, 258.

4 Siehe aber *Sydow*, in: Sydow, EU-Datenschutzgrundverordnung, Einl. Rn. 71; *Schulz*, in: Gola, DS-GVO, Art. 6 Rn. 9; *Buchner/Petri*, in: Kühling/Buchner, DS-GVO BDSG, Art. 6 Rn. 1 (abschließende und erschöpfende Aufzählung).

5 So eine Mitteilung des BMI, https://www.bmi.bund.de/SharedDocs/faqs/DE/themen/it-digitalpolitik/datenschutz/datenschutzgrundvo-liste.html.

6 BGH, Urt. v. 7.7.2020 – VI ZR 246/19, K&R 2020, 830, bestätigt vom BGH, Urt. v. 29.9.2020 –VI ZR 449/19, AfP 2020, 488.

7 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) v. 30.6.2017, BGBl. I, S. 2097.

8 Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2. DSAnpUG-EU) v. 20.11.2019, BGBl. I, S. 1626.

schutzrechts innerhalb der EU geführt hat.[9] Insofern trifft die Bemerkung zu, dass die DSGVO eher Richtliniencharakter habe (siehe Art. 94 Rn. 5).[10]

Auch unter der DSGVO wird das Datenschutzrecht vom Grundsatz des „**Verbots mit Erlaubnisvorbehalt**" geprägt. Ein gesetzliches Verbot im verwaltungsrechtlichen Sinn, das durch einen Verwaltungsakt aufzuheben wäre, enthält die Vorschrift, die als Verbotsadressaten auch die öffentlichen Stellen anspricht, nicht.[11] Die legislativen Ausnahmen vom Verbot ergeben sich unmittelbar aus dem Gesetz selbst. Soweit öffentliche Stellen personenbezogene Daten erheben, handelt es sich um einen Eingriff in das Datenschutzgrundrecht und bedarf einer gesetzlichen Legitimation; insoweit lässt sich von einem „Verbot mit *Eingriffs*vorbehalt" sprechen. Die Datenverarbeitung öffentlicher Stellen oder solcher, die öffentliche Aufgaben wahrnehmen, „bedarf einer detaillierten gesetzlichen Ermächtigung, die festlegt, unter welchen Bedingungen die Behörden zu welchem Zweck welche Daten erheben dürfen".[12] **4**

Das gilt nicht in gleicher Weise für die Verarbeitung durch Private, die nicht durch eine „**Eingriffserlaubnis**" legitimiert werden müsste. Zur Freiheit gehört die offene Kommunikation, das Sammeln und Verbreiten (auch) von personenbezogenen Daten. Dass die Datenverarbeitung durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten (Art. 2 Abs. 1 lit. c DSGVO) dem sachlichen Anwendungsbereich der DSGVO entzogen ist („household exemption" – **Haushaltsausnahme**) bringt dieses zum Ausdruck.[13] Gleichwohl hat der (europäische) Gesetzgeber aufgrund grundrechtlicher Schutzpflichten auch einen Ausgestaltungsauftrag, um Freiheitsrechte zu sichern. Wie in vielen anderen Rechtsbereichen, von denen nur das Verbraucherschutz- und AGB-Recht zu nennen sind, so gibt es auch beim Datenschutz im nicht-öffentlichen Bereich den Verfassungsauftrag, das Selbstbestimmungsrecht durch Regulierung zu wahren. Die technischen Möglichkeiten der Profilbildung, der personalisierten Big-Data-Auswertungen, der individuellen Beeinflussung von Wahl- und Marktverhalten auf der Grundlage von Auswertungen personenbezogener Daten, die in unvorstellbarem Ausmaß bei der Nutzung des elektronischen Fernabsatzes preisgegeben und die in Sozialen Medien verbreitet werden, erfordern gesetzliche Schutzmaßnahmen. Die Datensammlungen, -analysen und -nutzungen durch die sog. „Internetgiganten" aus kommerziellem und politischem Interesse rücken immer mehr in das öffentliche Bewusstsein, dass die **mittelbare Schutzwirkung der Grundrechte** für die Freiheitswahrnehmung ebenso weit gehen kann wie die unmittelbare. **5**

Das *Fraport*-Urteil des Bundesverfassungsgerichts erhellt, dass „je nach Gewährleistungsinhalt und Fallgestaltung die mittelbare Grundrechtsbindung Privater einer Grundrechtsbindung des Staates vielmehr nahe oder auch gleich kommen (kann). Für den Schutz der Kommunikation kommt das insbesondere dann in Betracht, wenn private Unternehmen die Bereitstellung schon der Rahmenbedingungen öffentlicher Kommunikation selbst über- **6**

9 Vgl. *Schaar*, vorgänge 221/222 (2018), 31, 37 („datenschutzrechtlichen Flickenteppich"); *Roßnagel*, vorgänge 221/222 (2018), 17, 22 f. (Ziel, einen soliden, kohärenten, einheitlichen Rechtsrahmen für den Datenschutz in allen Mitgliedstaaten der Union zu bilden, wurde verfehlt); *Laue*, ZD 2016, 463. Gegen den Vorwurf „Flickenteppich" wendet sich *Greve*, NVwZ 2017, 737.

10 Siehe etwa *Peifer*, PinG 2016, 222, 223.

11 Deshalb bevorzugt *Bäcker*, in: Wolff/Brink, BeckOK DatenschutzR, § 4 BDSG a. F. Rn. 1, den Begriff „Verbotsgrundsatz".

12 *Masing*, NJW 2012, 2305, 2306.

13 Kritisch zur Herausnahme aus dem Anwendungsbereich *Gola/Lepperhoff*, ZD 2016, 9, 12.

nehmen".[14] Daraus folgt auch die Pflicht des (europäischen) Gesetzgebers, den selbstbestimmten Umgang der betroffenen Person mit den sich auf seine Person beziehenden und beziehbaren Daten so zu regeln, dass das **Grundrecht auf Datenschutz auch in Privatrechtsbeziehungen** wirksam bleibt.[15] Die allgemeinen Grundsätze des Datenschutzes, wie sie in Art. 5 DSGVO festgelegt wurden und zu denen an erster Stelle die Pflicht zur Herstellung von Transparenz und Zweckbindung gehören, sind Ausdruck dieses Verfassungsverständnisses, das auch den (privaten) Verantwortlichen ausreichend Raum gewährt, ihre Grundrechte in einem fairen Ausgleich mit den Grundrechten der betroffenen Personen zur Geltung zu bringen. Es ist deswegen verfassungsrechtlich geboten, dass die DSGVO, die zunächst in den allgemeinen Regelungen zwischen öffentlichen und nicht-öffentlichen Stellen nicht (mehr) differenziert, ein **allgemeines Verbot mit Erlaubnisvorbehalt** statuiert. Mit Art. 6 Abs. 1 UAbs. 1 DSGVO und insbesondere mit der Erlaubnis nach Buchstabe f wird den Einzelfällen besonders in Privatrechtsverhältnissen durch Abwägung auch der Interessen der Verantwortlichen angemessen Rechnung getragen.

7 Wegen des auch weiter geltenden alternativlosen „Verbots mit Erlaubnisvorbehalt"[16] ist unabdingbare Voraussetzung für die Rechtmäßigkeit der in Art. 4 Nr. 2 DSGVO legaldefinierten Datenverarbeitung das Vorhandensein einer Erlaubnis durch eine Einwilligung oder durch eine der in Abs. 6 Abs. 1 UAbs. 1 lit. b bis f DSGVO vorgesehenen Erlaubnistatbestände. Für besondere Kategorien personenbezogener Daten enthält Art. 9 Abs. 1 DSGVO ein spezielles ausdrückliches Verbot („ist untersagt") mit den das Verbot zurücknehmenden Erlaubnistatbeständen in Abs. 2, der die Erlaubnistatbestände bei besonderen Kategorien personenbezogener Daten abschließend und ohne Rückgriffsmöglichkeit auf die allgemeinen Erlaubnistatbestände in Art. 6 Abs. 1 UAbs. 1 DSGVO regelt.[17] Das aus dem **Grundrecht auf Informationelle Selbstbestimmung** (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) folgende „Verbot der Verarbeitung personenbezogener Daten mit Eingriffsvorbehalt" und das aus dem § 4 Abs. 1 BDSG a.F. bekannte einfachgesetzliche „Verbot mit Erlaubnisvorbehalt" haben auch unter der DSGVO – trotz vereinzelter Kritik an diesem Grundsatz[18] – wei-

14 BVerfG, Urt. v. 22.2.2011 – 1 BvR 699/06, NJW 2011, 1201, Rn. 59 = BVerfGE 128, 226, 248 f.

15 Dagegen vehement *Veil*, NVwZ 2018, 686, 695, der meint, dass „das Verbot mit Erlaubnisvorbehalt im privaten Bereich zu einem Rechtfertigungszwang grundrechtlich geschützten Verhaltens" führe: „Kollateralschäden sind alle anderen Grundrechte. Das Datenschutzrecht folgt einer Abschottungslogik, die einseitig zulasten von Meinungs-, Presse-, Informations-, Kunst- und Wissenschaftsfreiheit sowie unternehmerischer Freiheit geht." Ähnlich auch *Bull*, Netzpolitik, S. 136.

16 Für die Beibehaltung bzw. Stärkung des Verbotsprinzips *Buchner/Schwichtenberg*, GuP 2016, 218, 219; *Albrecht*, CR 2016, 88, 91; *Spindler*, DB 2016, 937, 939; *Karg*, DuD 2013, 75; *Weichert*, DuD 2013, 246; *Buchner*, DuD 2016, 155, 157 f.; *Hornung*, ZD 2012, 99; *Heberlein*, in: Ehmann/Selmayr, DS-GVO, Art. 6 Rn. 1; *Buchner/Petri*, in: Kühling/Buchner, DS-GVO BDSG, Art. 6 Rn. 14; *Spindler*, Persönlichkeitsschutz im Internet, Gutachten F zum 69. DJT, S. 102. Vgl. auch *Brühann*, in: Grabitz/Hilf/Nettesheim, EU-Recht, Art. 7 DSRl Rn. 6.

17 Ebenso die Kommentierung hier von *Mester*, Art. 9 Rn. 2; *Schulz*, in: Gola, DS-GVO, Art. 9 Rn. 1; *Schiff*, in: Ehmann/Selmayr, DS-GVO, Art. 9 Rn. 9; *Kampert*, in: Sydow, EU-Datenschutzgrundverordnung, Art. 9 Rn. 63; a.A. *Weichert*, in: Kühling/Buchner, DSGVO, Art. 9 Rn. 4; *Robrahn/Bremert*, ZD 2018, 291, 295.

18 Den Grundsatz des Verbots mit Erlaubnisvorbehalt trotz der eindeutigen grundrechtlichen Vorgabe aus Art. 8 Abs. 2 Satz 1 GRCh ablehnend *Veil*, NVwZ 2018, 686, 688 f.; *Bull*, Netzpolitik, 2013, S. 136; *Nettesheim*/*Diggelmann*, VVDStRL 2011, 7; *Härting*, in: Taeger, IT und Internet, S. 687; *Härting/Schneider*, ZRP 2011, 233; *Härting*, AnwBl 2012, 716; *Härting*, BB 2012, 459; *Härting*, in: Leible/Kutschke, Schutz der Persönlichkeit im Internet, 2013, S. 55; *Härting/Schneider*, CR 2015, 819, 822; *Schneider*, ITRB 2011, 243; *Schneider*, AnwBl 2011, 233; *Schneider*, ITRB 2012,

terhin Bestand.[19] Art. 8 Abs. 2 Satz 1 GRCh bestimmt, dass die Daten von natürlichen Personen nur mit Einwilligung der betroffenen Person oder aufgrund einer sonstigen gesetzlich geregelten legitimen[20] Grundlage verarbeitet werden dürfen. Daher ist das Verbotsprinzip verfassungsrechtlich determiniert.[21] Auch wenn dieses Grundrecht primär ein Abwehrrecht gegen staatliche Eingriffe ist (Art. 51 GRCh), so folgt daraus auch die Pflicht des Gesetzgebers, den Datenschutz auch auf der Ebene der Privatrechtsbeziehungen zur Wirksamkeit zu verhelfen. Diesem Auftrag kommt die Verordnung mit Art. 6 DSGVO nach. Im Weiteren werden dann die vom Verantwortlichen entlang dem Pflichtenkatalog der DSGVO zu ergreifenden Maßnahmen davon abhängen, wie groß das Risiko für die Verletzung von Persönlichkeitsrechten der betroffenen Person eingeschätzt wird (risikobasierter Ansatz).[22] Ausgenommen von dem Verbot mit Erlaubnisvorbehalt ist nach Art. 2 Abs. 2 lit. c DSGVO allerdings die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten (**Haushaltsausnahme**; siehe oben Rn. 5 und Art. 2 Rn. 16 ff.).

Auf der Ebene des Sekundärrechts ist der (europäische) Gesetzgeber gehalten, die grundrechtlich geschützten Interessen von Verantwortlichen und betroffenen Personen durch einfachgesetzliche Vorschriften zum Ausgleich zu bringen.[23] Dies erfolgte auf Grundlage der **8**

180; *Schneider/Härting*, CR 2014, 306, 308; *Peifer*, K&R 2011, 543; *Giesen*, PinG 2013, 62; *Giesen*, NVwZ 2019, 1711, 1714 („Totalitäre Tendenz; Gefahr „totalitärer Phanasien"). Kritisch hinsichtlich dieses Schutzkonzepts im nicht-öffentlichen Bereich, das „rechtspolitisch, aber auch rechtsstaatlich bedenklich" sei, *Assion/Nolte/Veil*, in: Gierschmann/Schlender/Stentzel/Veil, DSGVO, Art. 6 Rn. 42, unter Hinweis auf *Stentzel*, PinG 2016, 45, und *Bull*, Sinn und Unsinn des Datenschutzes, S. 13.

19 Gegen die Verwendung der Begriffe wendet sich Widerspruch in der Sache: *Roßnagel*, NJW 2019, 1. Auch in der ePrivacy-Verordnung soll nach dem vorliegenden Entwurf des Art. 5 Satz 2 ePrivacyVO-E ein Verbot der Verarbeitung elektronischer Kommunikationsdaten mit Erlaubnisvorbehalt eingeführt werden. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) v. 29.1.2021, Rats-Dok. 5642/21.

20 Die Verwendung des Terminus „legitim" sowohl in Art. 8 Abs. 2 Satz 1 GRCh („auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet") als auch in Art. 5 Abs. 1 lit. b DSGVO weist darauf hin, dass die Rechtsgrundlage selbst verfassungsgemäß sein muss. Die Datenverarbeitung bedarf nicht nur eines Erlaubnistatbestands, sondern es ist zu gewährleisten, dass der Zweck nicht von der Rechtsordnung missbilligt wird; siehe dazu *Specht*, GRUR Int. 2017, 1040, 1042, m. w. N., sowie pointiert *Rost*, vorgänge 221/222 (2018), 79, 84 f.

21 Siehe auch *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, Art. 6 Rn. 1; *Sydow*, in: Sydow, EU-Datenschutzgrundverordnung, Einl. Rn 71; *Schulz*, in: Gola, DS-GVO, Art. 6 Rn. 2: Im Bereich der öffentlichen Hand „verlangen Prinzipien wie der Gesetzesvorbehalt und der Bestimmtheitsgrundsatz, dass jeder Eingriff in die Freiheit eines Einzelnen auf ein" formelles Gesetz rückführbar sein muss. Das Verbotsprinzip „ist Ausdruck dieser einer demokratischen Gesellschaft immanent zugrundeliegenden Dogmatik".

22 Siehe dazu schon *Veil*, ZD 2015, 347; *Bieker*, DuD 2018, 27; *Rost*, vorgänge 221/222 (2018), 79. Vgl. auch WP 248 der Art.-29-Datenschutzgruppe und das Kurzpapier Nr. 18 der Datenschutzkonferenz (DSK) „Risiko für die Rechte und Freiheiten natürlicher Personen", das eine Definition von Risiko geben und eine Methode zur Bestimmung von Risiken für die Rechte und Freiheiten natürlicher Personen und Bewertung der Rechtsfolgen aus dem Risiko aufzeigen will, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf.

23 Vgl. dazu ausführlich *Schulz*, in: Gola, DS-GVO, Art. 6 Rn. 3.

Datenschutzrichtlinie auch bislang schon durch nationales Recht mit dem **Verbot mit Erlaubnisvorbehalt** nach § 4 Abs. 1 BDSG a. F.

9 Einfachgesetzlich beginnt Art. 6 Abs. 1 DSGVO mit der Bedingung: „Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der [in Art. 1 UAbs. 1 lit. a bis f DSGVO] genannten Bedingungen erfüllt ist." Ist das nicht der Fall, ist die Verarbeitung personenbezogener Daten verboten, es sei denn, es ergeben sich Erlaubnistatbestände aus den Fachgesetzen, die aufgrund von **Öffnungsklauseln** neben oder anstelle der DSGVO zur Anwendung kommen, oder aus Erlaubnissen, die sich aus **Vorschriften außerhalb des Anwendungsbereichs der DSGVO** ergeben. Damit ist Art. 6 Abs. 1 DSGVO diejenige Vorschrift, aus der sich in der Regel eine Erlaubnis für die Verarbeitung personenbezogener Daten im sachlichen und räumlichen Anwendungsbereich der DSGVO (Art. 2 und 3 DSGVO) ergibt.

10 Die EU war zur Gewährleistung des in Art. 16 Abs. 1 AEUV (Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten) und des mit dem wortgleichen Art. 8 GRCh verbürgten **Grundrechts auf Datenschutz** angetreten, mit der DSGVO auf „rasche technologische Entwicklungen und die Globalisierung" (ErwG 6) zu reagieren, die den Datenschutz vor neue Herausforderungen gestellt haben. Im Fokus waren die weltweit agierenden Anbieter sozialer Medien und solche Unternehmen, die die Nutzer des Internets tracken und Profile anlegen. Gleichwohl macht die DSGVO jedenfalls bei den Erlaubnistatbeständen keinen Unterschied, ob ein globaler Konzern, ein lokaler Sportverein oder ein Handwerksbetrieb personenbezogene Daten verarbeitet. Ausnahmen bestehen etwa nur, wenn weniger als 250 Beschäftigte im Unternehmen tätig sind, sodass die Verpflichtung entfallen kann, ein Verzeichnis der Verarbeitungstätigkeiten zu führen (Art. 30 Abs. 5 DSGVO). Eine Differenzierung des Risikopotenzials findet auf dieser Ebene nicht statt. Zutreffend ist der Befund von *Roßnagel*: „*In keiner Regelung werden die spezifischen Grundrechtsrisiken z. B. von smarten Informationstechniken im Alltag, von Big Data, Cloud Computing oder datengetriebenen Geschäftsmodellen, Künstlicher Intelligenz und selbstlernenden Systemen angesprochen oder gar gelöst. Die gleichen Zulässigkeitsregeln, Zweckbegrenzungen oder Rechte der betroffenen Person gelten für die wenig riskante Kundenliste beim „Bäcker um die Ecke" ebenso wie für diese um Potenzen risikoreicheren Datenverarbeitungsformen. Insbesondere durch abstrakte Zulässigkeitsregelungen wie in Art. 6 Abs. 1 werden die spezifischen Grundrechtsrisiken verfehlt.*"[24]

11 Hinzu kommt, dass für nicht-öffentliche Verantwortliche neben der Erlaubnis aus einer Einwilligung oder wegen der Notwendigkeit, Daten zur Durchführung vorvertraglicher Maßnahmen oder zur Erfüllung vertraglicher Pflichten (Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO) vornehmlich die sehr weitreichende Erlaubnis aus Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO zur Verfügung steht, bei der der Verantwortliche eine Interessenabwägung vornimmt, mit der ein Mehr an Rechtssicherheit gegenüber der Situation unter dem BDSG a. F. nicht zu erwarten ist.[25] Es wird auf die Rechtsprechung und den **Europäischen Datenschutzausschuss** ankommen, hier Leitplanken einzuziehen. Immerhin erkennt die DSGVO das Problem, wenn sie zwar das Profiling selbst nicht regelt, es in ErwG 72 aber heißt, dass der nach Art. 68 DSGVO eingerichtete Europäische Datenschutzausschuss verbindliche Leitlinien zum Profiling herausgeben soll.

---

24 Vorgänge 221/222 (2018), 17, 24.

25 Deshalb ist der pointierten Kritik von *Schulz*, in: Gola, DS-GVO, Art. 6 Rn. 6, zuzustimmen.

Die Erlaubnistatbestände des Art. 6 DSGVO können nur in der Zusammenschau mit weiteren Vorschriften der DSGVO zu einer rechtmäßigen Verarbeitung führen. So sind die **Grundsätze aus Art. 5 DSGVO** stets mit zu berücksichtigen. Im Zusammenhang mit dem Erlaubnistatbestand der Einwilligung sind die Anforderungen an die Wirksamkeit der Einwilligung aus Art. 4 Nr. 11 und Art. 7 DSGVO zu beachten. Bei der im Zusammenhang mit der Anbahnung oder Durchführung eines Vertragsverhältnisses erforderlichen Verarbeitung der Daten von Kindern, die das 16. Lebensjahr nicht vollendet haben, ist zu bedenken, dass die Sorgeberechtigten gem. Art. 8 DSGVO ihre Einwilligung geben müssen, wenn ein Anbieter von Diensten in der Informationsgesellschaft die Vertragsdaten oder weitere Daten verarbeiten will, die nicht für den Vertragszweck erforderlich sind (siehe Art. 8 Rn. 24 ff.). **12**

Gehören die zu verarbeitenden Daten zu einer **besonderen Kategorie von Daten**, ist Art. 9 DSGVO heranzuziehen. Sollen die Daten in einen **Drittstaat** übermittelt werden, so hängt die Zulässigkeit der Datenverarbeitung davon ab, dass in einer zweiten Stufe der Zulässigkeitsprüfung die Anforderungen aus Art. 44 DSGVO erfüllt werden können (siehe Art. 44 Rn. 14 ff.). Will eine **Behörde** personenbezogene Daten für hoheitliche Zwecke verarbeiten, so hat sie Art. 6 Abs. 1 UAbs. 2 DSGVO zu beachten, der eine auf UAbs. 1 lit. f gestützte Verarbeitung ausschließt. **13**

2. Entstehungsgeschichte und bisherige Regelung

Eine mit Art. 6 Abs. 1 DSGVO vergleichbare Regelung fand sich in Art. 7 DSRl, in der ebenfalls das Verbot mit Erlaubnisvorbehalt vorgesehen und Erlaubnistatbestände genannt wurden.[26] **14**

3. Regelungszweck

Die Vorschrift führt die zentralen Erlaubnistatbestände auf, aufgrund derer die Rechtmäßigkeit der Verarbeitung personenbezogener Daten gegeben sein kann. Anders noch als das BDSG a. F. wird im Normtext nicht zwischen verschiedenen **Phasen der Datenverarbeitung** differenziert, sodass unter „Datenverarbeitung" nach der Legaldefinition des Art. 4 Nr. 2 DSGVO alle Phasen einer Verarbeitung einschließlich der Erhebung und Übermittlung zu verstehen sind, für die es jeweils eine Erlaubnis geben muss. Weitere Erlaubnisse können sich bei besonderen Kategorien aus Art. 9 Abs. 2 DSGVO ergeben. Daneben ist Art. 5 DSGVO zu beachten, der nicht nur die Rechtmäßigkeit der Verarbeitung voraussetzt, sondern auch weitere Anforderungen nennt, *wie* die Daten zu verarbeiten sind.[27] **15**

4. Normadressaten

Anders als noch im BDSG a. F. wird in der DSGVO grundsätzlich und im Wesentlichen nicht zwischen öffentlichen Stellen und nichtöffentlichen Stellen unterschieden; eine Ausnahme gibt es dort, wo aus verfassungsrechtlichen Gründen ein Eingriff durch eine hoheitliche Stelle auf einer Rechtsgrundlage beruhen muss, die hinreichend bestimmt ist (siehe **16**

26 Zu den Änderungen gegenüber Art. 7 DSRl und der Entstehungsgeschichte mit einem Vergleich der Entwurfsfassungen *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, Art. 6 Rn. 3 ff.

27 Siehe auch *Reimer*, in: Sydow, EU-Datenschutzgrundverordnung, Art. 6 Rn. 1.

Buchstaben c und e). Weil das bei der auf einer Abwägung von Interessen beruhenden Erlaubnis gem. Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO nicht der Fall ist, sieht UAbs. 2 vor, dass dieser Erlaubnistatbestand nicht für die von **Behörden in Erfüllung ihrer hoheitlichen Aufgaben** vorgenommene Verarbeitung gilt (siehe Rn. 121 f.). Siehe zu der Frage, ob und ggf. in welchem Umfang hoheitliche Stellen ihre Datenverarbeitung auf eine Einwilligung stützen können, die Kommentierung zu Art. 7 Rn. 21 ff.[28]

17 Sich nicht auf die Erlaubnis aus Art. 6 Abs. 1 UAbs. 1 lit. e Alt. 2 DSGVO können sich die nicht-öffentlichen Verantwortlichen (Private) berufen, weil dieser Erlaubnistatbestand denjenigen vorbehalten ist, bei denen „die Verarbeitung … für die Wahrnehmung einer Aufgabe erforderlich (ist), die … in **Ausübung öffentlicher Gewalt** erfolgt, die dem Verantwortlichen übertragen wurde".

18 Die Erlaubnistatbestände können auch von **Institutionen der Strafverfolgung und des Justizvollzugs** sowie von den für die Gefahrenabwehr zuständigen Behörden nicht in Anspruch genommen werden, für die Art. 8 RL (EU) 2016/680 bzw. die mitgliedstaatlichen Umsetzungsgesetze einschlägig sind. Das wären in Deutschland §§ 45 ff. BDSG und die einschlägigen Umsetzungsgesetze, die zumeist Bestandteil der Datenschutzgesetze der Länder sind. Die Organe der Europäischen Union finden Erlaubnistatbestände in Art. 5 VO (EG) 45/2001.

19 Ansonsten folgt aus der nunmehr weitgehend einheitlichen Regelung für öffentliche und nicht-öffentliche Verantwortliche, dass sowohl die nicht-öffentlichen wie die öffentlichen Verantwortlichen – unter vorgenannter Einschränkung – ihre Erlaubnis für die jeweils beabsichtigte Datenverarbeitung dem Art. 6 Abs. 1 UAbs. 1 DSGVO zu entnehmen haben, wenn die Tätigkeit des Verantwortlichen (Art. 4 Nr. 7 DSGVO) im Lichte des Art. 2 Abs. 2 DSGVO in den **sachlichen Anwendungsbereich** der Verordnung fällt. Neben den Verantwortlichen sind auch die Auftragsverarbeiter, die betroffenen Personen, die Aufsichtsbehörden, die Mitgliedstaaten und die Union Adressaten von Vorschriften der DSGVO.

II. Erlaubnistatbestände (Abs. 1)

20 Ist der Anwendungsbereich der DSGVO eröffnet, so finden sich die zentralen Erlaubnistatbestände in Art. 6 Abs. 1 UAbs. 1 DSGVO. Der Verantwortliche hat für jede Phase der Verarbeitung, die in der Legaldefinition des Art. 4 Nr. 2 DSGVO aufgeführt wird, und für den jeweiligen mit der Verarbeitung verfolgten Zweck die Erlaubnis anhand der Tatbestandsmerkmale der in Betracht gezogenen Erlaubnisnorm zu prüfen. Die Rechtmäßigkeit der Verarbeitung ist in allen vom Gesetz genannten Phasen (Art. 4 Nr. 2 DSGVO) vom Vorliegen einer Erlaubnis abhängig, auch schon die **Erhebung von Daten** (Art. 5 Abs. 1 lit. b DSGVO). Es wird aufgrund der Rechtsprechung des Bundesverfassungsgerichts auch unter der DSGVO und im Lichte des Art. 8 GRCh davon ausgegangen werden können, dass „ungezielt und allein technikbedingt zunächst miterfasste" und „unmittelbar nach der Signalaufbereitung technisch wieder spurenlos ausgesonderte" Daten vom Verbot nicht erfasst werden.[29]

---

28 *Reimer*, in: Sydow, EU-Datenschutzgrundverordnung, Art. 6 Rn. 15, meint allerdings, dass für den staatlichen Bereich bei Vorliegen einer Einwilligung schon der Schutzbereich des Art. 8 GRCh nicht gegeben sei.

29 BVerfG, Urt. v. 11.3.2008 – 1 BvR 2074/05, BVerfGE 120, 378, 433 = NJW 2008, 1505 m. w. N. (automatisierte Kennzeichenerfassung).

Art. 6 Abs. 1 UAbs. 1 erklärt es ausdrücklich für denkbar, dass **mehrere Erlaubnisnormen nebeneinander** bestehen können („*mindestens eine* der nachstehenden Bedingungen" muss erfüllt sein). Auch Art. 17 Abs. 1 lit. b DSGVO ist ein Argument dafür, dass die Verarbeitung auf mehrere Erlaubnistatbestände, zumindest auf einen Erlaubnistatbestand neben der Einwilligung, gleichzeitig gestützt werden kann. Dies hat auch der EuGH in der Rechtssache Fashion-ID bestätigt.[30] So kann nach dem Widerruf einer Einwilligung das Recht auf Löschung verwehrt werden, wenn die Erlaubnis zur Verarbeitung auch aus einer anderen Erlaubnis folgt.[31] **21**

Erfolgt die Datenverarbeitung zur **Erfüllung einer Rechtspflicht** (lit. c), so wird dies oft auch im Interesse des Verantwortlichen liegen (lit. f).[32] Der gleiche Erlaubnisgrund kann auch herangezogen werden, wenn die rechtmäßig verarbeiteten Daten zu einem anderen Zweck verarbeitet werden sollen, was nur bei der Erlaubnis aufgrund einer Einwilligung nicht möglich wäre. **22**

Bei allen Erlaubnistatbeständen von lit. b bis lit. f ist das „übergeordnete Prinzip"[33] der **Erforderlichkeit** zu beachten. Erforderlich ist die Datenverarbeitung nur, wenn eine Aufgabe oder ein Zweck ohne Verarbeitung der personenbezogenen Daten nicht oder nicht in zumutbarer Weise erfüllt werden kann (dazu näher Rn. 57 ff.). **23**

1. Einwilligung (lit. a)

An erster Stelle der Erlaubnistatbestände, aber keineswegs mehr so besonders hervorgehoben, wie es in § 4 Abs. 1 BDSG a. F. der Fall war,[34] steht die Einwilligung, die als „Schlüssel zu einem unbegrenzten Datenzugang" angesehen wird.[35] Es lässt sich keineswegs aus der Reihenfolge der Buchstaben a bis f eine **Rangfolge der Erlaubnistatbestände** ablesen,[36] zumal für nicht-öffentliche Verantwortliche neben dem Erlaubnistatbestand aus Buchstabe b (Vorvertragliche Maßnahmen; zur Vertragserfüllung) die Erlaubnis nach einer Interessenabwägung gemäß Buchstabe f von herausragender Bedeutung sein dürfte. Dieser Erlaubnistatbestand der Interessenabwägung wird auch als Generalklausel[37] bezeichnet und der Vorzug vor einer Einwilligungslösung gegeben, zumal die Einwilligung jederzeit **24**

30 EuGH, Urt. v. 29.7.2019 – C-40/17, K&R 2019, 562.

31 Siehe auch *Schwartmann/Jacquemain*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, Art. 6 Rn. 8; *Plath*, in: Plath, BDSG DSGVO, Art. 6 Rn. 5; *Remmertz*, GRUR-Prax 2018, 254; *Veil*, NVwZ 2018, 686. Es gibt kein „Primat der Einwilligung" (siehe aber *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 72).

32 *Reimer*, in: Sydow, EU-Datenschutzgrundverordnung, Art. 6 Rn. 8.

33 *Buchner/Petri*, in: Kühling/Buchner, DS-GVO BDSG, Art. 6 Rn. 15.

34 Vgl. *Reimer*, in: Sydow, EU-Datenschutzgrundverordnung, Art. 6 Rn. 8.

35 So *Kollmar/El-Auwad*, Grenzen der Einwilligung bei hochkomplexen und technisierten Datenverarbeitungen, in: Taeger, Den Wandel begleiten, S. 199, 202 f., 206. Siehe auch die Datenethikkommission, Gutachten vom 23.10.2019, S. 96: Der Einzelne ist systematisch überfordert, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.html.

36 Ebenso *Drewes*, CR 2016, 721, 723. Die zentrale Rolle der Einwilligung als Ausdruck des Selbstbestimmungsrechts betont *Tinnefeld*, vorgänge 221/222 (2018), 41.

37 *Reimer*, in: Sydow, EU-Datenschutzgrundverordnung, Art. 6 Rn. 6; *Assion/Nolte/Veil*, in: Gierschmann/Schlender/Stentzel/Veil, DSGVO, Art. 6 Rn. 22; *Bunnenberg*, JZ 2020, 1088, 1092; *Dallmann/Busse*, ZD 2019, 394, 399.

widerrufbar ist. Gleichwohl sollte aus der Relevanz der Norm keine Rangfolge abgeleitet werden.

25 Das bislang aus dem Allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) abgeleitete und nun auch aus Art. 8 GRCh folgende Datenschutzgrundrecht (Informationelles Selbstbestimmungsrecht) gewährleistet dem Einzelnen ein **umfassendes Selbstbestimmungsrecht** darüber, wer welche Daten über ihn zu welchem Zweck erhalten soll.[38] Art. 8 Abs. 2 Satz 1 GRCh betont, dass jeder über den Umgang mit personenbezogenen Daten selbst bestimmt und in die Datenverarbeitung einwilligen kann. Die Einwilligung ist daher ein „zentrales Instrument" des Schutzes der Persönlichkeit. Es ist nicht zu verkennen, dass die Grundrechtsträger gemeinschaftsgebundene Individuen sind. Das Bundesverfassungsgericht hatte deshalb bereits im Volkszählungsurteil[39] hervorgehoben, dass dieses Selbstbestimmungsrecht nicht schrankenlos gewährt wird, sondern auch ohne Einwilligung aufgrund einer verfassungsmäßigen gesetzlichen Erlaubnis personenbezogene Daten verarbeitet werden dürfen (Rn. 26).

26 Eine schrankenlose Selbstbestimmung des Betroffenen mit einer uneingeschränkten Verfügung über seine personenbezogenen Daten im öffentlichen und nicht-öffentlichen Bereich gibt es nicht. Auch das Recht auf informationelle Selbstbestimmung wird nicht schrankenlos gewährt. Das BVerfG hob dies in seinem Volkszählungsurteil hervor und betonte, dass der Einzelne kein Recht im Sinne einer absoluten, unbeschränkbaren Herrschaft über „seine" Daten hat, sondern dieser vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit sei. Information, auch soweit sie personenbezogen ist, stelle ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden könne.[40] Im Sinne der Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person müsse daher der Einzelne **Einschränkungen seines Rechts auf informationelle Selbstbestimmung** im überwiegenden Allgemeininteresse hinnehmen.

27 Mit dieser Einschränkung umfasst der Grundrechtsschutz die Befugnis des Einzelnen, über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen. Die Erteilung einer Einwilligung erweist sich so als **Grundrechtsausübung** und nicht etwa als Grundrechtsverzicht. Mit Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO und der darin vorgesehenen Möglichkeit, durch Einwilligung eine Erlaubnis in die Verarbeitung der personenbezogenen Daten zu schaffen, wird dieses Selbstbestimmungsrecht zum Ausdruck gebracht (Art. 7 Rn. 1).

28 Der europäische Gesetzgeber und – im Rahmen der Öffnungsklauseln und ihrer Regulierungskompetenz – die mitgliedstaatlichen Gesetzgeber dürfen daher auch aus verfassungsrechtlicher Perspektive im Lichte des Art. 8 GRCh abwägen, ob datenschutzrechtliche Erlaubnistatbestände im überwiegenden Allgemeininteresse oder im objektiven Eigeninteresse der betroffenen Person auch eine Verarbeitung ohne Einwilligung der betroffenen Person zulassen dürfen. Wenn keine Erlaubnis aufgrund eines Gesetzes besteht, kann die **Einwilligung als weitere Möglichkeit zur Legitimation** einer Verarbeitung eingeholt werden. Die Datenethikkommission sieht in der datenschutzrechtlichen Einwilligung

38 Siehe auch *Buchner/Petri*, in: Kühling/Buchner, DS-GVO BDSG, Art. 6 Rn. 17.
39 BVerfG, Urt. v. 23.12.1983 – 1 BvR 209/83, BVerfGE 65, 1 = NJW 1984, 419.
40 BVerfG, Urt. v. 23.12.1983 – 1 BvR 209/83, BVerfGE 65, 1, 43.

„einen zentralen Mechanismus zur Gewährleistung informationeller Selbstbestimmung im digitalen und analogen Bereich".[41]

Die Einwilligung setzt die selbstbestimmte, freie Entscheidung der betroffenen Person voraus, ob sie personenbezogene Daten über sich zur Verfügung stellen will und welche Daten zu welchem Zweck und an welchem Verarbeitungsort verarbeitet werden dürfen. So kann die Einwilligung in die Verarbeitung eingeschränkt, von Bedingungen abhängig gemacht oder befristet werden. **29**

a) Einwilligungsfähigkeit

Eine Einwilligung kann nur von solchen betroffenen Personen erteilt werden, die die erforderliche **Einsichtsfähigkeit** besitzen. Nur dann, wenn eine Einwilligung von einem Kind gefordert wird, das das 16. Lebensjahr noch nicht vollendet hat, und zudem die Einwilligungserklärung gegenüber einem **Dienst der Informationsgesellschaft** abgegeben werden soll, der ein Angebot (auch) einem Kind gegenüber macht, so sind die Anforderungen aus Art. 8 DSGVO zu beachten (Art. 8 Rn. 13 ff.).[42] Ist das nicht der Fall, findet Art. 8 DSGVO mit der Folge keine Anwendung, dass eine Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a i.V.m. Art. 7 DSGVO einzuholen ist oder sich die Erlaubnis nach einer das Alter des Kindes berücksichtigenden Abwägung gem. Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO ergibt.[43] **30**

Werden Daten von Kindern nicht von einem Dienst der Informationsgesellschaft verarbeitet, kommt es auf die Einsichtsfähigkeit an. **Volljährigkeit** ist nicht Voraussetzung. Die Einsichtsfähigkeit hinsichtlich möglicher Folgen einer Datenverarbeitung kann bei 16 Jahre alten Jugendlichen angenommen werden. Bei Jüngeren ist sie im Einzelfall der bezweckten Verarbeitung – also nicht gesondert im Fall eines betroffenen Jugendlichen – festzustellen. Im Einzelfall kann auch hinterfragt werden, ob die Einsichtsfähigkeit im hohen Alter noch besteht;[44] hier wäre der Anknüpfungspunkt in sehr seltenen Fällen dann aber das Individuum, wobei zu bedenken ist, dass von Verantwortlichen häufig weder das Alter erfragt wird, noch die individuelle Einsichtsfähigkeit prüfbar ist. **31**

b) Freiwilligkeit

Die Einwilligung erfordert gemäß Art. 4 Nr. 11 DSGVO eine „freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der **32**

41 Gutachten der Datenethikkommission, 2019, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6, S. 96.

42 Bisweilen wird übersehen, dass eine Einwilligung bzw. Zustimmung bei der Verarbeitung von Kindern bis zum 16. Lebensjahr nicht generell nach Art. 8 DSGVO zu geben ist, sondern nur dann, wenn sie von einem Dienst der Informationsgesellschaft für die Verarbeitung der für die Vertragserfüllung nicht erforderlichen Daten verlangt wird. Diese Prüfung fehlt etwa bei *Götz/Götz*, FamRZ 2020, 1250, 1251.

43 Siehe auch *Nelles*, ITRB 2021, 60.

44 Mit der Frage befasst sich *Janicki*, Die Einwilligungsfähigkeit zwischen Digitalisierung und demographischem Wandel, in: Taeger, Die Macht der Daten und der Algorithmen, S. 313. Siehe auch *Tinnefeld/Conrad*, ZD 2018, 391, 393.

die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist" (siehe auch Art. 4 Rn. 302). Freiwillig erfolgt die Einwilligungserklärung, wenn sie **ohne jeden Zwang oder Druck** abgegeben wurde und die betroffene Person bei einer Verweigerung der Einwilligung oder einen Widerruf keine Nachteile befürchten muss (Art. 7 Rn. 88 ff.).[45] Sachwidrige Kopplungen der Einwilligung mit anderen Erklärungen sind deshalb unzulässig (Art. 7 Rn. 94 ff.).

33 Eine Freiwilligkeit läge auch dann nicht vor, wenn zwar nicht vom Verantwortlichen, sondern von Dritten ein **gesellschaftlicher Druck** ausgeübt würde, der sich zu einem **sozialen Zwang** ausweiten könnte. So wurde erwogen, ob die „Publicity Kampagne" zur Nutzung der **Corona-Warn-App** (CWA) zu einer „faktischen sozialen Ächtung" führen könnte, wenn die CWA nicht heruntergeladen würde.[46] Würde man eine solche Zwangssituation bejahen, würde sie die Freiwilligkeit aufheben. Einen so starken Druck gab und gibt es bei der CWA allerdings nicht, sondern es wird vielmehr öffentlich stets auf die Freiwilligkeit der Nutzung hingewiesen. Auch Arbeitgeber dürfen die Nutzung der CWA nicht verlangen oder gar zur Voraussetzung für ein Betreten des Arbeitsplatzes machen. Im Übrigen findet bei einem Herunterladen einer App – abgesehen von den einem App Store bei der Installation übermittelten Daten – noch keine Datenverarbeitung statt, deren Rechtmäßigkeit einer Einwilligung bedürfte. Eine Datenverarbeitung durch die CWA auf der Grundlage einer Einwilligung wäre allenfalls bei einer Infektionsmeldung zu prüfen.[47]

34 Die Frage nach der Freiwilligkeit stellt sich eher bei der **Luca-App**, die der besseren Nachverfolgung der **Covid19-Infektionskette** dienen soll; weil die Nutzung der App als Voraussetzung für das Betreten von Geschäften, Gastronomiebetrieben und Freizeiteinrichtungen gemacht wird, ist der Druck erheblich größer, eine Einwilligung zu erteilen, weil mit ihrer Nutzung „positive Anreize für individuelle Personen" gesetzt werden.[48] Es müsste dann sogar eine *ausdrückliche* Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO sein, weil **Gesundheitsdaten** zu den besonderen Kategorien personenbezogener Daten gehören. Eine schon für die CWA geforderte Regulierung mit einer gesetzlichen Erlaubnis gibt es auch für die Luca-App nur teilweise in **Corona-Schutz-Verordnungen**. So hat die Sächsische Corona-Schutz-Verordnung vom 10.6.2021 in § 6 Abs. 7 und 8 Einrichtungen verpflichtet, vorrangig digitale Systeme für die Kontaktnachverfolgung zu verwenden, mit denen ausschließlich für den genannten Zweck Name, Telefonnummer oder E-Mail-Adresse und Anschrift der Besucher sowie Zeitraum und Ort des Besuchs verarbeitet werden dürfen.[49] Soweit keine Regelungen zur digitalen Erfassung von **Kontaktverfolgungsdaten** erfolgen, enthalten die Verordnungen der Länder Verpflichtungen, Besucherdaten in analogen Listen zu erfassen und zu dokumentieren. Eine Verpflichtung des Gastes, die Luca-App zu nutzen, folgt daraus nicht. Wenn sie eingesetzt wird, willigt die betroffene Person in die Verarbeitung ihrer personenbezogenen Gesundheitsdaten ein, weil die zunächst ver-

---

45 Ausführlich zu den Bedingungen der Freiwilligkeit *Haase*, InTeR 2019, 113.

46 Siehe dazu *Ruschemeier*, ZD 2020, 618, 620; *Müller*, MMR 2020, 355, 357 f.

47 *Kühling/Schildbach*, NJW 2020, 1545, 1549.

48 *Kühling/Schildbach*, NJW 2020, 1545, 1549.

49 SächsCoronaSchVO v. 29.3.2021 i.d. konsolidierten Fassung v. 16.4.2021, https://www.coronavirus.sachsen.de/download/SMS-Saechsische-Corona-Schutz-Verordnung-2021-06-10.pdf. Vgl. auch § 5 Abs. 1 Satz 7a Nds. Corona-Verordnung v. 30.5.2021 (Nds. GVBl. S. 297) in der aktuellen Fassung.